

REMARKS

Applicant's representative thanks the Examiner for the courtesies extended during the telephonic conference on October 17, 2007, with Francis Dunn. During the conference, there was discussion with regard to the Examiner's rejections under 35 U.S.C. §§ 101 and 103, as set forth in the Office Action, dated August 23, 2007. In particular, there was discussion of claims 1, as well as discussion of art cited by the Examiner in the Office Action, dated August 23, 2007, including Bresson, *et al.*, Provably Authenticated Group Diffie-Hellman Key Exchange, CCS'01, 2001, Philadelphia, Pennsylvania, USA, pp.255-264, and Della-Libera, *et al.*, Web Services Secure Conversation Language (<http://www.verisign.com/wss/WS-SecureConversation.pdf>).

Claims 1-22 are currently pending in the subject application and are presently under consideration. Claims 1, 2, 6, 13, 20, 21, 22 have been amended as shown on pages 4-7 of the Reply. In addition, the specification has been amended as indicated on pages 2-3.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1-22 Under 35 U.S.C. § 101

Claims 1-22 stand rejected under 35 U.S.C. § 101 because the claimed subject matter is directed to non-statutory subject matter. It is requested that this rejection be withdrawn for at least the following reason. The claimed subject matter as recited in claims 1-22 produces a useful, concrete, and tangible result and is therefore within the bounds of statutory subject matter in accordance with 35 U.S.C. § 101.

Title 35, section 101, explains that an invention includes "any new and useful process, machine, manufacture or composition of matter."... Without question, *software code alone qualifies as an invention eligible for patenting under these categories*. *Eolas Techs., Inc. v. Microsoft Corp.*, 399 F.3d 1325, 1338-39 (Fed. Cir. 2005) (holding that 35 U.S.C. § 101 did not limit inventions or components of an invention to structural or physical components (*e.g.*, non-software components). *Rather, every component, including software components, of every form of invention deserves the protection of § 271(f) because it is patentable subject matter under 35 U.S.C. §101*).

In particular, independent claim 1 (and similarly independent claims 13, 20, 21, and 22), as amended, recites: A *computer-implemented* communication system comprising:

a secure message generation system that employs a first dialog session key to encrypt a first message to be sent to a second service, the secure message generation system is associated with a first service; and

a secure message receiver system that employs a second dialog session key to decrypt a second message received from the second service, the secure message receiver system is associated with the first service, wherein the second dialog session key is created unilaterally by a secure message generation system associated with the second service in order to maintain secure message protocol and facilitate a reduction in latency in communications between the first service and the second service.

The claimed subject matter can be implemented by computers in a communication network and can facilitate secure messaging between a secure message receiver system of a first service and a secure message generation system of a second service. The secure message generation system can unilaterally shift the dialog session key, and can send a message encrypted based in part on the shifted dialog session key to the secure message receiver system of the first service, without having to negotiate with the first service or reaching an agreement with the first service with regard to the dialog session key. The secure message receiver system of the first service can decrypt the message based in part on the shifted dialog session key. As a result, the claimed subject matter, through the use of unilaterally created dialog session keys, can provide secure messaging between the first service and the second service in an efficient manner, as latency associated with communication between the first service and the second service can be reduced.

In view of at least the foregoing, the subject claims produce a useful, concrete, and tangible result and are properly limited to statutory subject matter in accordance with 35 U.S.C. §101. Therefore, it is believed that the subject claims are in condition for allowance, and withdrawal of this rejection is respectfully requested.

II. Rejection of Claims 1-22 Under 35 U.S.C. § 103(a)

Claims 1-22 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Helland (<http://www.microsoft.com/presspass/exec/flessner/04-11flessnerteched.msp>) (“hereinafter referred to as “Helland, *et al.*”), Bresson, *et al.*, Provably Authenticated Group Diffie-Hellman Key Exchange, CCS’01, 2001, Philadelphia, Pennsylvania, USA, pp.255-264 (hereinafter referred to as “Bresson, *et al.*”), and Rosenberg, *et al.*, Internet Engineering Task Force (<http://tools.ietf.org/html/draft-ietf-sip-rfc2543bis-09>, section 26) (hereinafter referred to as “Rosenberg, *et al.*”), and Della-Libera, *et al.*, Web Services Secure Conversation Language (<http://www.verisign.com/wss/WS-SecureConversation.pdf>) (hereinafter referred to as “Della-Libera, *et al.*”). It is requested that the rejection be withdrawn for at least the following reasons: Bresson, *et al.*, Helland, *et al.*, Rosenberg, *et al.*, and Della-Libera, *et al.*, either alone or in combination, do not disclose, teach, or suggest each and every element of the subject claims.

The prior art reference (or references when combined) ***must teach or suggest all claim limitations***. See MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant’s disclosure. See *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

The claimed subject matter relates to the unilateral shifting of dialog session keys utilized in the encryption and decryption of secure message between networked communication systems. In accordance with one aspect of the claimed subject matter, a first service can comprise a secure message generation system and a secure message receiver system; and a second service can comprise a secure message generation system and a secure message receiver system. A first service can generate a first dialog session key that can be utilized to encrypt a first message, which can be sent to the second service. The secure message generation system of the second service can unilaterally create a second dialog session key, without negotiating or reaching an agreement with the first service regarding the unilateral change to the second dialog session key, and can encrypt a second message based in part on the second dialog session key and can send the encrypted second message and the second dialog session key to the first service. The secure message receiver system of the first service can receive the encrypted second message and second dialog session key, and can decrypt the second message using the second dialog session

key. The claimed subject matter can thereby maintain secure message protocol in a relatively autonomous environment and can facilitate a reduction in handshaking between the first service and second service and/or a reduction in latency associated with the communication system.

In particular, independent claim 1 (and similarly independent claims 13, 20, 21, and 22), as amended, recites: *a secure message receiver system that employs a second dialog session key to decrypt a second message received from the second service, the secure message receiver system is associated with the first service, wherein the second dialog session key is created unilaterally by a secure message generation system associated with the second service in order to maintain secure message protocol and facilitate a reduction in latency in communications between the first service and the second service.* Bresson, *et al.*, Rosenberg, *et al.*, Helland, *et al.*, and Della-Libera, *et al.*, either alone or in combination, do not teach or suggest such distinctive features of the claimed subject matter.

Rather, Bresson, *et al.* teaches of a formal model to assess Group Diffie-Hellman protocols for Authenticated Key Exchange (AKE), which are used to provide multicast message integrity for a pool of players over an open network, using a shared secret key. (*See* p.255, sec. 1, lines 1-5.) Bresson, *et al.* teaches the use of the Group Diffie-Hellman algorithm and construction of a model to determine success of various methods employing the Diffie-Hellman algorithm. (*See* pp.259-262, sec. 6.) The model is used to assess achievement of the fundamental security goal of each player being assured that no other player, aside from the arbitrary pool of players, can learn any information about the shared session key. (*See* p.255, sec. 1, para. 4, lines 1-6.) Various types of attack are modeled along with the model being extended to encompass the issues associated with mutual authentication. (*See* p.262, sec. 7.) However, unlike the claimed subject matter, Bresson, *et al.* fails to teach the use of unilateral shifting of dialog session keys to facilitate secure messaging of networked systems without negotiation and mutual agreement between two services in communication in a network.

Turning to Rosenberg, *et al.*, Rosenberg, *et al.* teaches various considerations for secure messaging *via* networks including an examination of threat models, security services required to address the threats, and mechanisms that can be used to provide the security services. (*See* p.242, sec. 26, para. 3.) Rosenberg *et al.* refers to “dialog session” in regard to the integrity of a dialog session between devices and the prevention of the dialog session being torn down prematurely through the use of forged BYE dialog session requests, as part of a third-party

attack. (See p.245, sec. 26.1.4., para. 1, line 2.) However, Rosenberg, *et al.* is silent regarding the generation and use of *unilateral* dialog session keys. Instead, Rosenberg, *et al.* simply refers to the use of a “session key” in discussion of modification of a session key by a malicious routing proxy server. (See p.244, sec. 26.1.3., para. 3, line 1.)

Helland, *et al.* also fails to teach the distinctive functionality of the claimed subject matter. Rather, Helland, *et al.* teaches of the concept of fiefdom and the autonomous nature of devices in networks, whereby each device does not trust any other device and acts autonomously with communications between each device being enabled through the use of an emissary, such as Web Services. (See para. 85-94.) Helland, *et al.* teaches that Web Services is designed to connect autonomous devices to facilitate point-to-point communication. (See para. 75-78.) Helland, *et al.* also teaches that the fiefdoms do not trust the emissary and will only accept messages and requests as long as they conform with the established Web Services messaging protocol. (See para. 92-96.) However, unlike the claimed subject matter, Helland, *et al.* fails to teach a service that can unilaterally create a dialog session key, without negotiation and agreement with another service, can encrypt a message with the unilaterally created key, and can send the encrypted message and unilaterally created key to the other service, where the other service can decrypt the message using the unilaterally created key.

Referring to Della-Libera, *et al.*, Della-Libera, *et al.* teaches Web Services-Security (WS-Security) specifications and mechanisms, including new message headers and SOAP extensions, to facilitate the establishment and sharing of security context and session key derivation, particularly for message authentication. (See Sec. 1.) Della-Libera, *et al.* teaches that the establishment of secure security context of exchange multiple messages is outlined through the use of a security token and derived keys along with the syntax of parameters and their coding to comply with the Web Services Secure Conversation Language specification. (See Sec. 3, para. 1.) Della-Libera, *et al.* teaches each party defining different key derivations to use, and the other party being able to derive the keys needed to use in the service. (See Sec. 5, para. 2.) However, unlike the claimed subject matter, Della-Libera, *et al.* fails to teach of dialog session keys being created by endpoints unilaterally.

In contrast, the claimed subject matter can facilitate the unilateral shifting of dialog session key(s) by a service sending a message to another service in a secure communication environment. In one aspect, a first service can send a message to a second service using a dialog

session key (*e.g.*, first dialog session key). In another aspect, when the second service sends a second message to the first service, the secure message generation system of a second service can ***unilaterally*** generate a different dialog session key (*e.g.*, second dialog session key), without having to negotiate and/or reach agreement with the first service with regard to the unilateral change in the dialog session key. The secure message can encrypt the second message using the unilaterally created second dialog session key, and can send the encrypted second message and the second dialog session key to the first service (*e.g.*, secure message receiver system of the first service), where the first service can decrypt the second message using the second dialog session key. The claimed subject matter can thereby maintain secure communication between the first service and second service (and other services) in the communication network, while reducing latency in the communication system, as for example, handshaking between the first service and second service associated with communication protocols can be reduced.

In view of at least the foregoing, Bresson, *et al.*, Rosenberg, *et al.*, Helland, *et al.*, and Della-Libera, *et al.*, either alone or in combination, do not disclose, teach, or suggest each and every element as recited in the independent claims 1, 13, 20, 21, and 22 (and associated dependant claims 2-4, 6-12, and 14-19). Accordingly it is believed that the subject claims are in condition for allowance, and rejection should be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP623US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROCY & CALVIN, LLP

/Himanshu S. Amin/

Himanshu S. Amin

Reg. No. 40,894

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731